Journal of Communications Technology, Electronics and Computer Science, Issue 9, 2016
ISSN 2457-905X

MackDroid - An Android based Application to monitor devices

Akshit Batheja[1], Aishwarya Kourani[1], Ekta Sirwani[1], Maaz Sirkhot[1], Kajal Jewani[2]
BE Students, Department of Computer Engineering, Vivekanand Education Society's Institute of Technology, Mumbai-400074, India[1]
Professor, Department of Computer Engineering, Vivekanand Education Society's Institute of Technology, Mumbai-400074, India[2]
akshit.batheja@ves.ac.in, aishwarya.kourani@ves.ac.in, ekta.sirwani@ves.ac.in, maaz.sirkhot@ves.ac.in, kajal.jewani@ves.ac.in

***Abstract*—In this technological world, smartphones can be considered as one of the most far-reaching inventions. It plays a vital role in connecting people socially. The number of mobile users using an Android based smartphone has increased rapidly since last few years resulting in organizations, cyber cell departments, government authorities feeling the need to monitor the activities on certain targeted devices in order to maintain proper functionality of their respective jobs. Also with the advent of smartphones, Android became one of the most popular and widely used Operating System. Its highlighting features are that it is user friendly, smartly designed, flexible, highly customizable and supports latest technologies like IoT. One of the features that makes it exclusive is that it is based on Linux and is Open Source for all the developers. This is the reason why our project Mackdroid is an Android based application that collects data from the remote device, stores it and displays on a PHP based web page. It is primarily a monitoring service that analyzes the contents and distributes it in various categories like Call Logs, Chats, Key logs, etc. Our project aims at developing an Android application that can be used to track, monitor, store and grab data from the device and store it on a server which can be accessed by the handler of the application.**

Keywords—Android; PHP; monitoring software

I. Introduction

MackDroid is an android monitoring system that allows complete control over the handset of the user by an elementary step installation process. It acquires all the important information as soon as it is installed on the host device. MackDroid is monitoring software which is divided into 2 parts: Client side and Server side. The client side consists of the mobile application which gets installed in the user's device and the server side consists of a database to store the information collected as well as the PHP website to access it. As soon as the application gets installed in the user's device, it connects with the server side through the internet. The prerequisites of this android application are a working internet connection, enabled location services and a smart phone having android version 4.0 and above. On the server side, requirements include a database to store all the collected data and a working computer to access the analyzed information through a web browser.

II. Literature Survey Review

A. Existing Systems and their drawbacks

Previous work emphasizes on breaching the loopholes in Android which is based on Linux kernel. The vulnerabilities in the kernel are very much universal in terms of exploitation by the attackers. It proposes to develop an application to exploit this vulnerability by developing an application containing a malware which runs legally on the device using permissions. The application will ask for permissions and by seeking all the permissions. This application runs a Trojan known as Remote Access Trojan aka RAT which steals the information such as call records, photos, videos and SMS. The Trojan will be a normal APK file that can be installed on Android device using Package Installer. In the source code of this application, there is a section where the attacker configures the URL of the C&C server, it is encoded with base64, the password is for the database that will be uploaded when the server receives information of the victim. The backup URL is in case the server was unavailable. Hence, this android application can potentially collect private information from the devices. Since, this application asks for all the permissions that are provided by the Android architecture, the detection of such malwares in Android device can be easily found out by checking the list of permissions and categorizing them into categories provided by the (ParvezFaruki, Ammar Bharmal, Vijay Laxmi, Vijay Ganmoor, Manoj Singh Gaur, Mauro Conti and MuttukrishnanRajarajan, «Android Security: A Survey of Issues, Malware Penetration and Defenses», IEEE Communications Surveys & Tutorials 2015, Volume: 17, Issue: 2 pp. 998 – 1022) in the paper. The 4 categories given are Normal, Dangerous, Signature and System permissions. [5]

An employee monitoring system already exists that is used to track the activities of the employees in the organization. It stores calls, messages, pictures, videos, browser cache etc on a central database which can be accessed by the manager. This application forms a secure connection between the devices using AES method. In this system, the device of the employee is connected to a 3g terminal so that the data is transferred to the manager application. The manager can therefore check the logs and activities to know if the employee has misused the device provided by the employer. This requires the two devices

of the manager and employee to be paired in order to exchange data. In order to overcome the limitations imposed by Bluetooth and Wi-Fi connections, this works on pairing between two devices on a web server. Also, whenever the data is to be transferred from one application to another, employee's device is connected by a 3g terminal by the employer and only then the data can be stored and transferred on to the server. [7]

Mobile activity monitoring system uses android as front end and My SQL as back end. This system sends all the call details and SMS details to the administrator as an alert as soon as the activity is performed by the android user. Location of the user can be checked anytime. And if the user crosses any geographical area, the administrator is alerted. The system alerts the administrator on each and every activity of the user, this can result in many redundant data and this data will be waste as it is of no use to the administrator if the user is not doing anything unethical. The system sends the message alerts from the user's device itself, this will lead to the user coming to know about the application and hence authentic data about the activity will not be available. Another shortcoming of this system is that it will be available for use to everyone which can lead to the unethical use of this system. The system discussed in this paper tracks the calls, SMS and location, but nowadays with growing popularity of IMs and Internet voice and video call services, this system might fail. [6]

The existing systems propose that the application should work as a Trojan or a spy and acquire the permissions from the device. Some systems propose to store the data on a server; some propose to alert the administrator as soon as any activity is performed while some make use of an encrypted channel to transfer the data to the administrator. The existing systems acquire the required permissions at once. This makes the systems susceptible to detection from antivirus. The existing systems show up in the application drawer of the device hence letting the user know about the application. This defies the main purpose of the application. The systems already in existence are readily available for use. This may lead to the unethical use of the application by criminals.

B. New Prosposed System

The detection of this malware can be verily made tougher by asking for only the set of permissions that are required for the application to perform a specific task. At no given point of time, the application should seek all the permissions as the processes running for each task will be different. Thereby, no independent process will have access full permissions [5]. This is to prevent the system from alerting the employee about the number of permissions used thereby antivirus or any permissions control algorithm does not detect tracking of the device data. As a result, we propose to develop a solution which needs no authorization or pairing from the employee's device. In fact, the application will have a stealth mode feature which hides the background processes of the application from the task manager window. Hence, enabling it to prevent the employee from having any knowledge about the malware installed on the device. This helps in getting the actual results and data from the employee's data [7]. To overcome the redundancy of the unwanted data, the administrator must be given an option to set certain rules. These rules will determine the tracking and storing of the required data only. Only when these rules are executed, the administrator will be alerted. The proposed system is developed with an option of a stealth mode and hence no alerts are sent from the user's device itself when the feature is turned on. The administrator is alerted through emails from the server about the relevant data and notifications. To prevent the unethical distribution and usage of this system, this solution can be installed and distributed over a valid purchase license only. [6]

MackDroid overcomes the drawbacks of existing solutions by providing the salient features such as permission distribution and management. For example, if the location has to be accessed, then only the permission for location access will be granted. MackDroid works in a stealth mode too. This feature helps to hide the application from the device users so that the authentic details of the activities can be collected. If anyone wants to use MackDroid, that person or an organization has to register and purchase a valid license. Using this license only, the application can be bought and installed on a particular device.

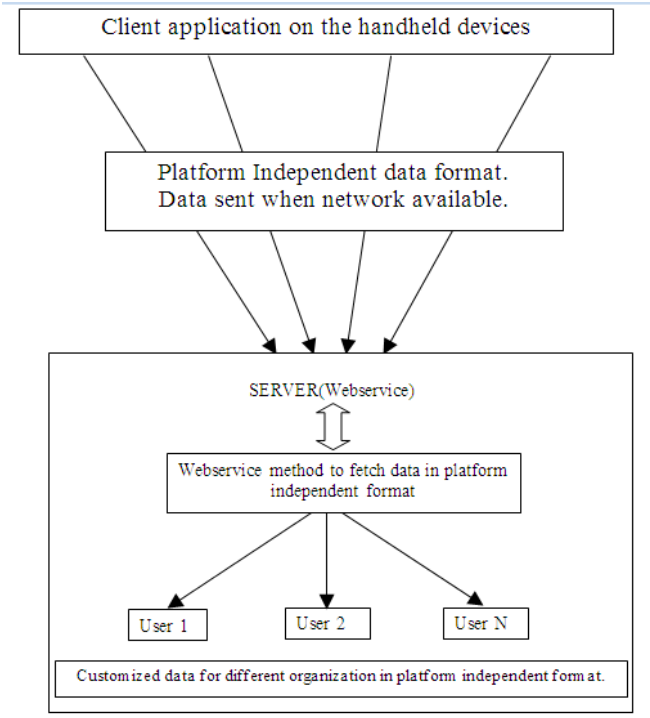

Fig. 1. Proposed System

III. System Design

MackDroid comprises of two main components- MackDroid android application and MackDroid web-panel. MackDroid android application will be developed using Android Studio and Eclipse. MackDroid web panel will be developed using PHP scripting language. MackDroid web-panel is connected to a remotely located server. This server

will be used to store user's data. The android application is connected to a local data store. The data from the mobile device is directly sent to the server when the device has internet connection. When the device is unable to connect to the internet, it stores the data locally in the local data store and transfers the data to the server when the internet gets activated.

MackDroid web panel will allow the users to register and purchase for new licenses. Once the user has successfully registered and has purchased a valid license, he/she will be provided with the MackDroid android application. This application will then be installed and will be ready for monitoring. Each and every user on registration is allotted a unique ID and password. This unique ID and password will ensure security and will ensure that no one other than the intended people have access to the highly sensitive data.

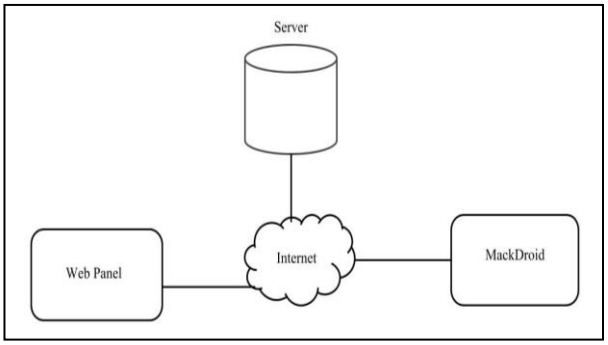

Fig. 2. System Design

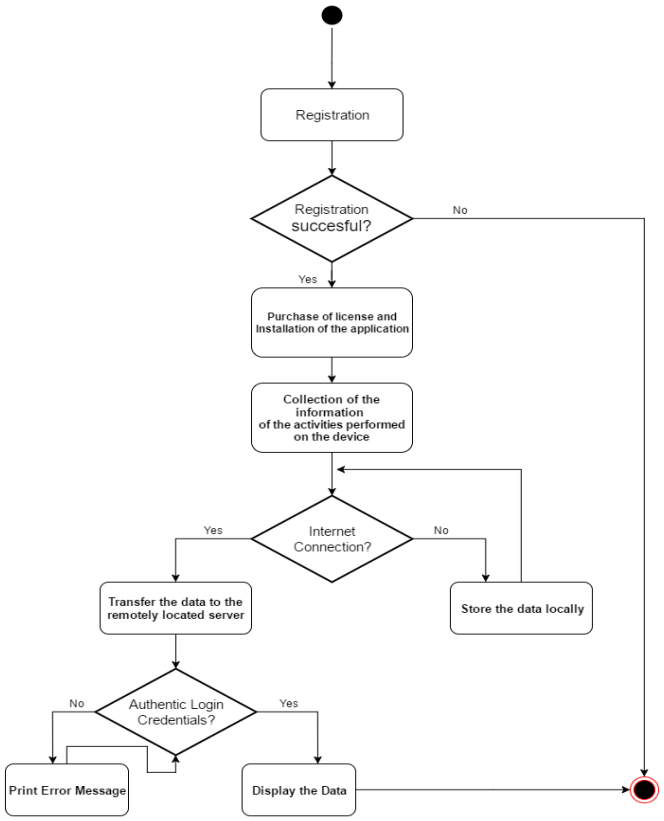

Fig. 3. System Flowchart

IV. System Requirements

A. Functional Requirements

1) A stand-alone android application to collect data from the user's device and store remotely.
2) The above client application can be used on Android version 4.0 and above and should run fine.
3) This application will be licensed application and will be provided to the Organizations as per their need. Every organization will have one unique profile assigned which will have all the information of the employees of that Organization. (Licensing is a method by which only the authorized users will be licensed to use the application. These authorized personals will have to purchase these licenses from time to time. Licensing is done by the Google Play Licensing server).
4) The stored data should be platform independent to be sent to the remote server.
5) The remote server should be able to collect data from various applications simultaneously and stored in the appropriate folder of each user.
6) When connected to a network, the client app should authenticate into a central server automatically and submit all the collected information.
7) The central server should verify the user and the information header before uploading the data to the database.

B. Non- functional Requirements

1) The data stored can be encrypted to protect from other Organisation profiles or by server theft.
2) Validating the platform independent format before inserting it into the centralized server (database).
3) This application will have another mode of operation (Stealth Mode) where the application will not be visible in the application manager of the device and will show no RAM Usage.
4) The performance with the server website will be high enough to handle simultaneous transactions by the users.

V. Future Scope

A. Stealth Mode Advancement

The stealth mode previously discussed in the proposed system doesn't support rooted devices. Future advancement involves an update which can hide the application even if the handler of the device is a SuperUser.

B. Increasing the reach of the application

Currently our application will only be available to companies and firms with proper registration and licence

purchase. The target audience can be further increased by making it commercially available on the Google Playstore.

VI. Conclusion

As we have observed that all the developed similar products have some loopholes, MackDroid has an upper hand as it not only overcome the drawbacks but also comes with various features which are not included in the other similar products.

Currently there is no application that provides complete monitoring of the mobile device. As Android is more popular and widely used than iOS, it is efficient to launch the Android application first. By weighing all the options for developing MackDroid web portal, the best is to use PHP for our server as PHP is more advantageous compared to other languages like HTML, .NET for the implementation of a database.

Acknowledgment

We are working on this project under the guidance of our Industry Mentor Mr. Yasir Arafat Shaikh (CEO & Founder, Macksofy Technologies) and our Institution Mentor Ms. Kajal Jewani (Assistant Professor, VESIT).

References

[1] www.ijircce.com/upload/2016/may/96_10_**Employee**.pdf
[2] www.ijarcce.com/upload/2015/february-15/IJARCCE3E.pdf
[3] ieeexplore.ieee.org/abstract/document/7529383
[4] https://www.quora.com/What-is-the-key-advantage-of-Android-over-other-mobile-operating-systems
[5] http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7529383
[6] http://www.ijarcce.com/upload/2015/february-15/IJARCCE3E.pdf
[7] http://www.ierjournal.org/vol1iss2/Employee%20Monitoring%20System%20Using%20Android%20Smartphone.pdf